Problem Set 7: Functional Verification

Hints and Notes

1. Given

P1 = while x>1 do x := x-1; z := z∗x end_while

P2 = while x>=1 do z := z∗x; x := x-1 end_while

P3 = while x<>1 do z := z∗x; x := x-1 end_while

f1 = (x>1 -> x, z := 1, zx! | x=1 -> I)

f2 = (x≥1 -> x, z := 1, z(x-1)! | x<1 -> I)

f3 = (x>1 -> x, z := 0, zx! | x=1 -> x, z := 0, z
| x<1 -> I)

Determine the correctness relationship between each program and function (C = Complete and Sufficient, S = Sufficient Only, N = Neither).

P1:

while x>1 do x := x-1; z := z*x end_while

P1:

```
while x>1 do x := x-1; z := z*x end_while
        x>1 -> x,z := ?, ?
```

P1:

```
while x>1 do x := x-1; z := z*x end_while
    x>1 -> x,z := 1, ?
```

P1:

```
while x>1 do x := x-1; z := z*x end_while
      x>1 -> x,z := 1,z(x-1)(x-2)...(1)
```

P1:

while x>1 do x := x-1; z := z*x end_while

x>1 -> x,z := 1,z(x-1)(x-2)...(1)

:= 1,z(x-1)!

P1:

```
while x>1 do x := x-1; z := z*x end_while
        x>1 -> x,z := 1,z(x-1)(x-2)...(1)
                   := 1,z(x-1)!
        x=1 -> x,z := ?, ?
```

P1:

```
while x>1 do x := x-1; z := z*x end_while
        x>1 -> x,z := 1,z(x-1)(x-2)...(1)
                    := 1,z(x-1)!
        x=1 -> x,z := x,z   (I)
```

P1:

```
while x>1 do x := x-1; z := z*x end_while
        x>1 -> x,z := 1,z(x-1)(x-2)…(1)
                   := 1,z(x-1)!
        x=1 -> x,z := x,z   (I)
                   := 1,z
```

P1:

```
while x>1 do x := x-1; z := z*x end_while
        x>1 -> x,z := 1,z(x-1)(x-2)...(1)
                   := 1,z(x-1)!
        x=1 -> x,z := x,z   (I)
                   := 1,z
                   := 1,z(1)
```

P1:

while x>1 do x := x-1; z := z*x end_while

x>1 -> x,z := 1,z(x-1)(x-2)...(1)

:= 1,z(x-1)!

x=1 -> x,z := x,z (I)

:= 1,z

:= 1,z(1)

:= 1,z(x-1)!

P1:

```
while x>1 do x := x-1; z := z*x end_while
        x>1 -> x,z := 1,z(x-1)(x-2)…(1)
                   := 1,z(x-1)!
        x=1 -> x,z := x,z   (I)
                   := 1,z
                   := 1,z(1)
                   := 1,z(x-1)!
        x<1 -> x,z := x,z   (I)
```

P1:

while x>1 do x := x-1; z := z*x end_while

x>1 -> x,z := 1,z(x-1)(x-2)…(1)

:= 1,z(x-1)!

x=1 -> x,z := x,z (I)

:= 1,z

:= 1,z(1)

:= 1,z(x-1)!

x<1 -> x,z := x,z (I)

p1: (x≥1 -> x,z := 1,z(x-1)! | true -> I)

P1:

```
while x>1 do x := x-1; z := z*x end_while
        x>1 -> x,z := 1,z(x-1)(x-2)...(1)
                    := 1,z(x-1)!
        x=1 -> x,z := x,z   (I)
                    := 1,z
                    := 1,z(1)
                    := 1,z(x-1)!
        x<1 -> x,z := x,z   (I)

p1: (x≥1 -> x,z := 1,z(x-1)! | true -> I)
                    or
    (x>1 -> x,z := 1,z(x-1)! | true -> I)
```

2. Use the correctness condition for sequencing to prove f = [P] where $f = (x, y := x+2, y(x^2+2x))$ and P is: $y := y*x$; $x := x+2$; $y := y*x$

2. Use the correctness condition for sequencing to prove $f = [P]$ where $f = (x, y := x+2, y(x^2+2x))$ and P is: $\underbrace{y := y*x}_{S1};\ \underbrace{x := x+2}_{S2};\ \underbrace{y := y*x}_{S3}$

2. Use the correctness condition for sequencing to prove f = [P] where $f = (x, y := x+2, y(x^2+2x))$ and P is: $y := y*x$; $x := x+2$; $y := y*x$

S1 **S2** **S3**

Therefore, P = **S1**; **S2**; **S3**. Does f = **s3** o **s2** o **s1**?

4. a. Determine the function of the following program.

```
temp := x
x := y
y := temp
if temp>z then
    y := z
    z := temp
    if x>y then
        temp := x
        x := y
        y := temp
    end_if
end_if
```

4. a. Determine the function of the following program.

```
        temp := x
        x := y          S1
        y := temp
        if temp>z then
            y := z
            z := temp
            if x>y then
S2              temp := x
                x := y
                y := temp
            end_if
        end_if
```

4. a. Determine the function of the following program.

```
temp := x
x := y
y := temp
if temp>z then
    y := z
    z := temp
    if x>y then
        temp := x
        x := y
        y := temp
    end_if
end_if
```

S1

S2.1

S2

S2.2

4. a. Determine the function of the following program.

```
            temp := x
            x := y              S1
            y := temp
            if temp>z then
                y := z              S2.1
                z := temp
S2              if x>y then
                    temp := x
       S2.2.1       x := y              S2.2
                    y := temp
                end_if
            end_if
```

4. a. Determine the function of the following program.

```
          temp := x
          x := y                S1
          y := temp                         [P] = [S2] o [S1]
          if temp>z then
              y := z                S2.1
              z := temp
S2            if x>y then
                  temp := x
      S2.2.1      x := y                    S2.2
                  y := temp
              end_if
          end_if
```

4. a. Determine the function of the following program.

```
          temp := x
          x := y              S1
          y := temp
          if temp>z then
              y := z          S2.1
              z := temp
S2            if x>y then
                  temp := x
S2.2.1            x := y      S2.2
                  y := temp
              end_if
          end_if
```

[P] = [S2] o [S1]

[S2] = (temp>z -> [S2.2] o [S2.1]
| temp≤z -> I)

4. a. Determine the function of the following program.

```
temp := x
x := y
y := temp
if temp>z then
    y := z
    z := temp
    if x>y then
        temp := x
        x := y
        y := temp
    end_if
end_if
```

S1

S2.1

S2

S2.2.1

S2.2

[P] = [S2] o [S1]

[S2] = (temp>z -> [S2.2] o [S2.1]
| temp≤z -> I)

[S2.2] = ...

5. For program A below, hypothesize a function *a* for [A] and prove *a* = [A].

```
while x<y+b do
   x := x+2
   y := y+1
end_while
```

You may assume that the function of the while_do body, G, is:

$$g = (x, y, b := x+2, y+1, b)$$

5. What is *a?*

while x<y+b do x := x+2; y := y+1 end_while

5. What is *a?*

while x<y+b do x := x+2; y := y+1 end_while

x<y+b -> x, y, b := ?, ?, ?

5. What is *a?*

while $x<y+b$ do $x := x+2; \; y := y+1$ end_while

$$x<y+b \rightarrow x, y, b := x+2(y+b-x), y+(y+b-x), b$$

5. What is *a?*

while $x<y+b$ do $x := x+2;\ y := y+1$ end_while

$$x<y+b \rightarrow x, y, b := x+2(y+b-x), y+(y+b-x), b$$
$$:= -x+2y+2b, -x+2y+b, b$$

5. What is *a?*

while $x<y+b$ do $x := x+2;\ y := y+1$ end_while

$$x<y+b \rightarrow x, y, b := x+2(y+b-x), y+(y+b-x), b$$
$$:= -x+2y+2b, -x+2y+b, b$$

$$x=y+b \rightarrow x, y, b := ?, ?, ?$$

5. What is *a?*

while x<y+b do x := x+2; y := y+1 end_while

x<y+b -> x, y, b := x+2(y+b-x), y+(y+b-x), b

:= -x+2y+2b, -x+2y+b, b

x=y+b -> x, y, b := x, y, b

5. What is *a?*

while $x<y+b$ do $x := x+2;\ y := y+1$ end_while

$$x<y+b \;\text{->}\; x, y, b := x+2(y+b-x),\ y+(y+b-x),\ b$$
$$:= -x+2y+2b,\ -x+2y+b,\ b$$

$$x=y+b \;\text{->}\; x, y, b := x, y, b$$
$$:= -x+2y+2b,\ -x+2y+b,\ b$$

5. What is *a?*

while $x<y+b$ do $x := x+2$; $y := y+1$ end_while

$x<y+b$ -> $x, y, b := x+2(y+b-x), y+(y+b-x), b$
$:= -x+2y+2b, -x+2y+b, b$

$x=y+b$ -> $x, y, b := x, y, b$
$:= -x+2y+2b, -x+2y+b, b$

$x>y+b$ -> $x, y, b := x, y, b$

5. What is *a*?

while $x<y+b$ do $x := x+2$; $y := y+1$ end_while

$$x<y+b \rightarrow x, y, b := x+2(y+b-x), y+(y+b-x), b$$
$$:= -x+2y+2b, -x+2y+b, b$$

$$x=y+b \rightarrow x, y, b := x, y, b$$
$$:= -x+2y+2b, -x+2y+b, b$$

$$x>y+b \rightarrow x, y, b := x, y, b$$

Therefore, the hypothesized *a* =

$$(x\leq y+b \rightarrow x, y, b := -x+2y+2b, -x+2y+b, b \mid true \rightarrow I)$$

5. What is *a*?

while x<y+b do x := x+2; y := y+1 end_while

x<y+b -> x, y, b := x+2(y+b-x), y+(y+b-x), b
:= -x+2y+2b, -x+2y+b, b

x=y+b -> x, y, b := x, y, b
:= -x+2y+2b, -x+2y+b, b

x>y+b -> x, y, b := x, y, b

Therefore, the hypothesized *a* =

(x≤y+b -> x, y, b := -x+2y+2b, -x+2y+b, b | true -> I)

or equivalently,

(x**<**y+b -> x, y, b := -x+2y+2b, -x+2y+b, b | true -> I)

5. What is *a*?

while $x<y+b$ do $x := x+2; y := y+1$ end_while

$$x<y+b \text{ -> } x, y, b := x+2(y+b-x), y+(y+b-x), b$$
$$:= -x+2y+2b, -x+2y+b, b$$

$$x=y+b \text{ -> } x, y, b := x, y, b$$
$$:= -x+2y+2b, -x+2y+b, b$$

$$x>y+b \text{ -> } x, y, b := x, y, b$$

Therefore, the hypothesized *a* =

$(x\leq y+b \text{ -> } x, y, b := -x+2y+2b, -x+2y+b, b \mid true \text{ -> } I)$

or equivalently,

$(x<y+b \text{ -> } x, y, b := -x+2y+2b, -x+2y+b, b \mid true \text{ -> } I)$

You can choose the one that is easier to work with!

6. For program C below, hypothesize a function *c* for [C] and prove *c* = [C].

```
y := 1
k := 0
repeat
    y := y*2
    k := k+1
until k=n
```

6. What is *c?*

```
y := 1
k := 0
repeat
    y := y*2
    k := k+1
until k=n
```

6. What is *c?*

$$\begin{array}{l} \mathbf{C1} \left\{ \begin{array}{l} \text{y := 1} \\ \text{k := 0} \end{array}\right. \\ \mathbf{C2} \left\{ \begin{array}{l} \text{repeat} \\ \quad \left.\begin{array}{l} \text{y := y} * \text{2} \\ \text{k := k+1} \end{array}\right\} \mathbf{G} \\ \text{until k=n} \end{array}\right. \end{array}$$

6. What is *c?*

$$\mathbf{C1}\left\{\begin{array}{l}y := 1\\ k := 0\end{array}\right.$$

$$\mathbf{C2}\left\{\begin{array}{l}\text{repeat}\\ \qquad\left.\begin{array}{l}y := y*2\\ k := k+1\end{array}\right\}\mathbf{G}\\ \text{until } k=n\end{array}\right.$$

C = C1; C2

6. What is *c?*

$$
\begin{array}{ll}
\mathbf{C1}\left\{\begin{array}{l} \mathrm{y := 1} \\ \mathrm{k := 0} \end{array}\right. & \\
\mathbf{C2}\left\{\begin{array}{l} \mathrm{repeat} \\ \quad \left.\begin{array}{l} \mathrm{y := y*2} \\ \mathrm{k := k+1} \end{array}\right\} \mathbf{G} \\ \mathrm{until\ k=n} \end{array}\right. &
\end{array}
$$

C = C1; C2

c1 = [C1] = (y,k := 1,0) by observation

6. What is *c?*

$$
\begin{array}{l}
\mathbf{C1}\left\{\begin{array}{l} y := 1 \\ k := 0 \end{array}\right. \\
\mathbf{C2}\left\{\begin{array}{l} \text{repeat} \\ \qquad \left.\begin{array}{l} y := y*2 \\ k := k+1 \end{array}\right\}\mathbf{G} \\ \text{until } k=n \end{array}\right.
\end{array}
$$

C = C1; C2

c1 = [C1] = (y,k := 1,0) by observation
c2 = [C2] = (k<n -> y,k :=y2$^{\mathbf{n-k}}$,n) by hypothesis

6. What is *c?*

```
      y := 1
C1    k := 0
      repeat
           y := y*2
C2         k := k+1      G
      until k=n
```

C = C1; C2

c1 = [C1] = (y,k := 1,0) by observation
c2 = [C2] = (k<n -> y,k :=y2$^{\mathbf{n-k}}$,n) by hypothesis

Therefore, the hypothesized *c* = [C] = *c2* o *c1*

6. What is *c?*

$$\begin{array}{l} \mathbf{C1} \left\{ \begin{array}{l} y := 1 \\ k := 0 \end{array}\right. \\ \mathbf{C2} \left\{ \begin{array}{l} \text{repeat} \\ \qquad \left.\begin{array}{l} y := y*2 \\ k := k+1 \end{array}\right\} \mathbf{G} \\ \text{until } k=n \end{array}\right. \end{array}$$

C = C1; C2

c1 = [C1] = (y,k := 1,0) by observation

c2 = [C2] = (k<n -> y,k :=y$2^{\mathbf{n-k}}$,n) by hypothesis

Therefore, the hypothesized *c* = [C] = *c2* o *c1*

= (k<n -> y,k := y$2^{\mathbf{n-k}}$,n) o (y,k := 1,0)

6. What is *c?*

$$\begin{array}{l} \mathbf{C1}\left\{\begin{array}{l} y := 1\\ k := 0\end{array}\right. \\ \mathbf{C2}\left\{\begin{array}{l} \text{repeat}\\ \qquad \left.\begin{array}{l} y := y*2 \\ k := k+1\end{array}\right\}\mathbf{G} \\ \text{until } k=n\end{array}\right. \end{array}$$

C = C1; C2

$c1$ = [C1] = (y,k := 1,0) by observation

$c2$ = [C2] = (k<n -> y,k := $y2^{\mathbf{n-k}}$,n) by hypothesis

Therefore, the hypothesized c = [C] = $c2$ o $c1$

= (k<n -> y,k := $y2^{\mathbf{n-k}}$,n) o (y,k := 1,0)

= (n>0 -> y,k := $2^{\mathbf{n}}$,n)

Problem Set 7: Functional Verification

Hints and Notes